UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,313	04/08/2004	Jeff Steven Edgett	2062.024US1	9716

21186   7590   12/28/2007
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
12/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/821,313	EDGETT ET AL.
Office Action Summary	Examiner	Art Unit	
	Longbit Chai	2131	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 October 2007</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1 and 3-35</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1 and 3-35</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>08 April 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

1.   Presently, pending claims are 1 and 3 – 35.

Continued Examination Under 37 CFR 1.114

2.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

10/24/2007 has been entered.

Response to Argument

3.   Applicant's arguments with respect to instant claims have been fully considered

but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as
set forth in section 102 of this title, if the differences between the subject matter sought to be
patented and the prior art are such that the subject matter as a whole would have been obvious at
the time the invention was made to a person having ordinary skill in the art to which said subject
matter pertains. Patentability shall not be negatived by the manner in which the invention was
made.

4.   Claims 1 and 3 – 35 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Grootwassink (U.S. Patent 7,031,705), in view of Albert et al. (U.S. Patent

2003/0177389).

As per claim 1 and 30, Grootwassink teaches a method comprising:

performing, in a service access provider, operations including:

receiving an access request from a client access device (the mobile unit sends a

registration request to a serving MSC when roaming into a VLR (Grootwassink: Column

5 Line 35 – 47 and Column 4 Line 12 – 20: Examiner notes (a) a VLR is interpreted as a

first service access provider and (b) the registration to a VLR is just like a log-in process

for accessing to a computer system and hence is equivalent to access request to a

VLR, which can allow or denies the service request accordingly (Grootwassink: Column

4 Line 20)), the access request requesting access to <u>a packet-switched computer</u>

<u>network</u>, wherein a user associated with the client access device is a subscriber of a

second service access provider (Grootwassink: Column 2 Line 47 – 67 and Column 1

Line 15 – 41: (a) a HLR is qualified as a second service access provider while a VLR as

a first service access provider <u>(b) mobile wireless communication network is indeed</u>

<u>implemented as a message-based packet switching network technology to handle the</u>

<u>messages exchanged between the provider and the clients</u>);

establishing a communications link with the client access device to authenticate

and authorize the user (Grootwassink: Column 2 Line 47 – 67);

receiving client device configuration data from the client access device over the

communications link during an authentication and authorization exchange (Column 5

Line 35 – 47, Column 2 Line 63 – 67 / Line 48 – 62 and Column 5 Line 3 – 10: Examiner

notes the broadest and reasonable claim interpretations are made, according to MPEP

2111, such that a registration information is interpreted as a part of the device

configuration data);

transmitting the client device configuration data destined for the second service

access provider, wherein the second service access provider is operable to process the

client device configuration data (Grootwassink: Column 2 Line 47 – 67).

Grootwassink does not disclose expressly processing the client device

configuration data includes determining if the client device configuration data meets

predetermined security requirements.

Albert teaches processing the client device configuration data includes

determining if the client device configuration data meets predetermined security

requirements (Albert: Para [0067] Line 7 – 10 and [0066] & Figure 3: the user's

individual security setting associated with the client device is qualified as client device

configuration data and the corporate security policies is considered as predetermined

security requirements).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Albert within the system of Grootwassink

because (a) Grootwassink teaches providing a security validation for a roamer including

personal communication service (PCS) units in a wireless network (Grootwassink :

Column 1 Line 25 – 28 / Line 34 – 40 and Column 2 Line 6 – 10) and (b) Albert teaches

providing enhanced authenticating method by using the security enforcement module

that applies access security policy for regulating access at a client device including

mobile computer users in a wireless network (Albert: Para [0008] Line 4 – 13 and Para

[0024]).

Albert in view of Grootwassink teaches:

selectively granting the client access device access to the network based upon

the client device configuration data (Grootwassink: Column 2 Line 43 – 54 / Line 63 –

67) & (Albert: Para [0067] Line 7 – 10 and [0066] & Figure 3); and

receiving an indication about whether the client access device is granted access

to the network, the indication originating from the second service access provider

(Grootwassink: Column 2 Line 63 – 67 and Column 3 Line 2 – 4: the grant indication

originating from the HLR (i.e. the second service access provider) and accessing the

network via the VLR of the local network) & (Albert: Para [0067] Line 7 – 10 and [0066]

& Figure 3).

As per claim 3, Grootwassink as modified teaches determining if the client device

configuration data meets predetermined security requirements includes comparing the

client device configuration data with reference configuration data (Grootwassink:

Column 2 Line 63 – 67) & (Albert: Para [0067] Line 7 – 10 and [0066] & Figure 3).

As per claim 6, Grootwassink as modified teaches the establishing of the

communications link with the client access device includes, communicating an agent to

the client access device, the agent operable to identify the client device configuration

data and to communicate the client device configuration data to a server of the network

(Grootwassink: Column 2 Line 47 – 67 and Column 5 Line 6 – 10: the VLR

communicates the client configuration data with the HLR) & (Albert: Para [0067] Line 7 –

10 and [0066] & Figure 3).

As per claim 9, Grootwassink as modified teaches the establishing of the

communications link with the client access device includes communicating a command

set, which includes at least one command, to the client access device, the command set operable to identify the client device configuration data and to communicate the client device configuration data to a server of the network (Grootwassink: Column 2 Line 47 – 67 and Column 5 Line 6 – 10: a command set, for example, is to find out the wireless unit's identification (or registration information)) & (Albert: Para [0067] Line 7 – 10 and [0066] & Figure 3).

As per claim 13, Grootwassink as modified teaches after establishing communications with the client access device, authenticating a user associated with the client access device (Grootwassink: Column 2 Line 47 – 67 and Column 5 Line 6 – 10) & (Albert: Para [0067] Line 7 – 10 and [0066] & Figure 3).

As per claim 14, Grootwassink as modified teaches authenticating the user includes verifying user login information associated with the user attempting access to the network (Grootwassink: Column 2 Line 20 – 25 and Column 5 Line 6 – 10) & (Albert: Para [0067] Line 7 – 10 and [0066] & Figure 3).

As per claim 16, Grootwassink as modified teaches a system to verify configuration data of a client access device requesting access to a network, the system comprising:

a first service access provider (Grootwassink: Column 2 Line 33 – 46: a VLR is qualified as as a first service access provider), coupled to a network, to establish a communications link to the client access device to receive, from the client access device, authentication information for a user associated with the

client access device (Grootwassink: Column 5 Line 35 – 47 and Column 2 Line

63 – 67) and to receive the configuration data from the client access device over

the communications link during an authentication and authorization exchange

(Grootwassink: Column 5 Line 35 – 47, Column 2 Line 63 – 67 / Line 48 – 62 and

Column 5 Line 3 – 10: Examiner notes the broadest and reasonable claim

interpretations are made, according to MPEP 2111, such that a registration

information is interpreted as a part of the device configuration data); and

a second service access provider to receive the authentication information

and the configuration data from the first service access provider, to process the

configuration data, and to selectively grant the client access device access to the

network based upon the configuration data (Grootwassink: Column 2 Line 63 –

67 and Column 3 Line 2 – 4: the grant indication originating from the HLR (i.e.

the second service access provider) and accessing the network via the VLR of

the local network).

However, Grootwassink does not teach processing the configuration data

includes determining if the configuration data meets predetermined security

requirements.

Albert teaches processing the configuration data includes determining if

the configuration data meets predetermined security requirements (Albert: Albert:

Para [0067] Line 7 – 10 , Para [0066], [0025], [0072] and [0085] – [0098] & Figure

3: (a) the user's individual security setting associated with the client device is qualified

as client device configuration data and the corporate security policies is considered as

predetermined security requirements and (b) the corporate security policies that are

predefined and assigned to the user are typically downloaded to the user's

device from an integrity server).

It would have been obvious to a person of ordinary skill in the art at the

time the invention was made to combine the teaching of Albert within the system

of Grootwassink because (a) Grootwassink as modified teaches providing a security

validation for a roamer including personal communication service (PCS) units in

a wireless network (Grootwassink : Column 1 Line 25 – 28 / Line 34 – 40 and

Column 2 Line 6 – 10) and (b) Albert teaches providing enhanced authenticating

method by using the security enforcement module that applies access security

policy for regulating access at a client device including mobile computer users in

a wireless network (Albert: Para [0008] Line 4 – 13 and Para [0024]).

As per claim 32 and 34, Grootwassink teaches a method to manage

access to a network from a client access device, the method comprising:

requesting access to the network, the requesting involving a first service

access provider and a second service access provider (Grootwassink: Column 5

Line 35 – 47 and Column 2 Line 33 – 67: a HLR is qualified as a second service

access provider while a VLR as a first service access provider);

authenticating a user associated with the client access device in an

authentication and authorization exchange, wherein the user is a subscriber of

the second service access provider (Grootwassink: Column 5 Line 35 – 47 and Column 2 Line 33 – 67: the user is a subscriber of the HLR);

communicating client device configuration data to the second service access provider via the first service access provider (Grootwassink: Column 5 Line 35 – 47, Column 2 Line 63 – 67 / Line 48 – 62 and Column 5 Line 3 – 10: Examiner notes the broadest and reasonable claim interpretations are made, according to MPEP 2111, such that a registration information is interpreted as a part of the device configuration data);

receiving a verification response from the second service access provider via the first service access provider (Grootwassink: Column 2 Line 63 – 67: the indication originating from the HLR (i.e. the second service access provider)); and

if the user is authenticated and the verification response from the second service access provider indicates acceptance of the client device configuration data, accessing the network via the first service provider (Grootwassink: Column 2 Line 63 – 67 and Column 3 Line 2 – 4: the grant indication originating from the HLR (i.e. the second service access provider) and accessing the network via the VLR of the local network).

However, Grootwassink does not teach processing the configuration data, by the second service access provider, wherein processing configuration data includes determining if the configuration data meets predetermined security requirements.

Albert teaches processing the configuration data, by the second service access provider, wherein processing configuration data includes determining if the configuration data meets predetermined security requirements (Albert: Para [0067] Line 7 –10, Para [0066], [0025], [0072] and [0085] – [0098] & Figure 3: (a) the user's individual security setting associated with the client device is qualified as client device configuration data and the corporate security policies is considered as predetermined security requirements and (b) the corporate security policies that are predefined and assigned to the user are typically downloaded to the user's device from an integrity server and (c) HLR is the home service provider (i.e. 2nd service provider) of the mobile unit and evidently the HLR can include "the integrity server" (as taught by Albert) for enhanced security check of configuration data – This is also consistent with the disclosure of the instant specification that indicates including a configuration server (i.e. integrity server) to process the client device configuration data such that it can determine if the configuration data meets predetermined security requirements (SPEC: PG-PUB / Para [0013])).

Same rationale of combination applies herein as above in rejecting the claim 16.

As per claim 4 and 19, Grootwassink does not disclose expressly the second service access provider is further operable to update the client device configuration data if the client device configuration data fails to meet the predetermined security requirements.

Albert teaches the second service access provider is further operable to

update the client device configuration data if the client device configuration data

fails to meet the predetermined security requirements (Albert: Para [0066],

[0025], [0072] and [0085] – [0098] & Figure 3: the corporate security policies that

are predefined and assigned to the user are typically downloaded to the user's

device from an integrity server).

Same rationale of combination applies herein as above in rejecting the claim

16.

As per claim 5 and 20, Grootwassink as modified teaches selectively

granting the client access device access to the network includes, denying

access to the network if the client device configuration data is not updated

(Albert: [0066] & Figure 3: the last sentence).

As per claim 7 and 22, Grootwassink does not disclose expressly if after

the processing of the client device configuration data the client device

configuration data requires an update, using the agent to update the client

access device with updated configuration data.

Albert teaches if after the processing of the client device configuration

data the client device configuration data requires an update, using the agent to

update the client. access device with updated configuration data (Albert: Para

[0066], [0025], [0072] and [0085] – [0098] & Figure 3: the corporate security

policies that are predefined and assigned to the user are typically downloaded to the user's device from an integrity server).

Same rationale of combination applies herein as above in rejecting the claim 16.

As per claim 8 and 23, Grootwassink as modified teaches after updating the client access device, receiving an update result indicator from the agent to confirm that the configuration of the client access device has been updated (Albert: Para [0072]).

As per claim 10 and 25, Grootwassink does not disclose expressly if after the processing of the client device configuration data the client device configuration data requires an update, using the command set to update the client access device with updated configuration data.

Albert teaches if after the processing of the client device configuration data the client device configuration data requires an update, using the command set to update the client access device with updated configuration data (Albert: Para [0066], [0025], [0072] and [0085] – [0098] & Figure 3: the corporate security policies that are predefined and assigned to the user are typically downloaded to the user's device from an integrity server).

Same rationale of combination applies herein as above in rejecting the claim 16.

As per claim 11 and 27, Grootwassink as modified teaches the command set further includes a first command set to identify and communicate the client device configuration data to the server (Grootwassink: Column 2 Line 47 – 67 and Column 5 Line 6 – 10: a command set, for example, is to find out the wireless unit's identification (or registration information)), and a second command set to update the client access device with the updated configuration data ((Albert: Para [0066], [0025], [0072] and [0085] – [0098] & Figure 3: the corporate security policies that are predefined and assigned to the user are typically downloaded to the user's device from an integrity server).

As per claim 12 and 26, Grootwassink as modified teaches after updating the client access device, receiving an update result indicator from the client access device to confirm that the configuration of the client access device has been updated (Albert: Para [0096] – [0098] & Figure 3).

As per claim 15, 29 and 31, Grootwassink does not disclose expressly the client device configuration data includes at least one of virus definition data, firewall configuration data, and operating system configuration data.

Albert teaches the client device configuration data includes at least one of virus definition data, firewall configuration data, and operating system configuration data (Albert: Para [0090]: a message sent by the of client security module is a "firewall" event control related configuration data)

Same rationale of combination applies herein as above in rejecting the claim 16.

As per claim 17, Grootwassink as modified teaches processing the client device configuration data includes determining if the client device configuration data meets predetermined security requirements (Grootwassink: Column 2 Line 63 – 67).

As per claim 18, Grootwassink as modified teaches determining if the client device configuration data meets predetermined security requirements includes comparing the client device configuration data with reference configuration data (Grootwassink: Column 2 Line 63 – 67).

As per claim 21, Grootwassink as modified teaches the establishing of the communications link with the client access device includes, communicating an agent to the client access device, the agent operable to identify the client device configuration data and to communicate the client device configuration data to a server of the network (Grootwassink: Column 2 Line 47 – 67 and Column 5 Line 6 – 10: the VLR communicates the client configuration data with the HLR).

As per claim 24, Grootwassink as modified teaches the establishing of the communications link with the client access device includes communicating a command set, which includes at least one command, to the client access device,

the command set operable to identify the client device configuration data and to

communicate the client device configuration data to a server of the network

(Grootwassink: Column 2 Line 47 – 67 and Column 5 Line 6 – 10: a command

set, for example, is to find out the wireless unit's identification (or registration

information)).

As per claim 28, Grootwassink as modified teaches after establishing

communications with the client access device, authenticating a user associated

with the client access device (Grootwassink: Column 2 Line 47 – 67 and Column

5 Line 6 – 10).

As per claim 33 and 35, Grootwassink does not disclose expressly prior to

receiving a verification response, updated configuration data is received from the

network access system to replace the client device configuration data.

Albert teaches prior to receiving a verification response, updated

configuration data is received from the network access system to replace the

client device configuration data (Albert: Para [0066] Para [0097] and [0098]: the

integrity server updates and installs the security policies on the client device and

may deny the client's access to the network if the required security policy or

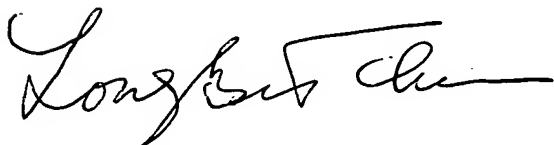module is not subsequently activated by the client device).

Same rationale of combination applies herein as above in rejecting the

claim 16.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Patent Examiner
Art Unit 2131
11/21/2007